CONSORTIA RISK MANAGEMENT STANDARDS

Background

To exercise due diligence HHSDC SAWS Oversight staff reviewed selected industry standards to obtain input to the process of establishing a "SAWS-wide" standard for consortium risk management. The following standards were reviewed:

- Standard for Software Project Planning (IEEE Std 1058-1998)
- Standard for Software Quality Assurance (QA) Plans (IEEE Std 730-1998)
- IEEE Guide for Software Quality Assurance Planning (IEEE Std 730.1-1995)
- Standard for Software Verification and Validation (V&V) (IEEE Std 1012-1998)
- IEEE Guide - Adoption of PMI Standard - A Guide to the Project Management Body of Knowledge (PMBOK) (IEEE Std 1490-1998)

These standards, with the exception of IEEE Std 1490-1998 (PMBOK), while requiring a risk management plan, provide little guidance with respect to the content of such a plan. The Standard for Software Project Planning (IEEE Std 1058-1998), provides a twelve line description of the requirements for a risk management plan. In addition, this standard refers to the SEI Continuous Risk Management Guidebook as a key reference for risk management planning. IEEE Std 1490-1998 (PMBOK) provides an eleven page description of risk management practices. The generic approach described is consistent with the other IEEE standards and with the SEI model.

SAWS project risk assessments used a variety of "checklist" type tools to assist in the assessment of risk, consistent with IEEE Std 1490-1998, Adoption of the PMI Standard, A Guide to the Project Management Body of Knowledge, Section 11.1.2.1. One of the key checklists used was the Software Engineering Institute (SEI) Taxonomy-Based Questionnaire, based on their Taxonomy of Software Risk. SEI risk management materials are recommended for use by IEEE (See, for example Std 1058-1998).

Consortia Standards

Each consortium must have a risk management plan and process and a tool to document and manage the process.

The plan must follow one of the accepted industry standards, as noted above, and contain the following elements:

Identify

Search for and locate risks before they become problems. Identify risks and set project priorities to arrive at a joint understanding. Identify new risks and changes.

Analyze

Process risk data into decision-making information to determine what is important to the project, to set priorities, and to allocate resources. Group risks and quantify impact, probability, and timeframe. The documented process must include an explanation of how probability and severity values are assigned

Plan

Translate risk information into decisions and mitigating actions (both present and future), and implement those actions. Joint risks require a team process to develop mitigation plans. Establish the mitigation plans for the risks. The risk strategy for a specific risk can take many forms: Eliminate, Mitigate, Accept, Study, or Transfer.

- Eliminate – The risk is immediately acted on. This is based on the cost of eliminating the risk versus the cost of potential impact and the likelihood that it will occur.
- Mitigate – Reduce the impact of the risk and the likelihood that the risk will occur to an acceptable level should the risk occur.
- Accept – Accept the consequence of it happening. This is an appropriate strategy for a low risk or a risk which have been mitigated to an acceptable level should the risk occur.
- Study – Resources are needed to further investigate the risk to acquire more information and better determine its characteristics to enable more knowledgeable decision-making.
- Transfer – The authority and accountability to actually deal with the risk lies elsewhere.

Track

Monitor risk indicators and mitigation plans. Indicators and trends provide information to activate plans and contingencies. These are also reviewed periodically to measure progress and identify new risks. Maintain visibility of risks, project priority, and mitigation plans.

Control

Correct for deviations from the risk mitigation plans. Actions can lead to corrections in products or processes. Any action may lead to joint resolution. Changes to risks, risks that become problems, or faulty plans require adjustments in plans or actions.

Communicate
Provide information and feedback internal and external to the project on the risk activities, current risks, and emerging risks. Communication occurs formally as well as informally. Establish continuous, open communication.

In addition, each consortium must have a formal risk management process that is documented. The process should include regularly scheduled meetings with representatives from the appropriate sections of the project team (e.g., county functional staff, county technical staff, vendor staff).

The CalWIN Approach

The CalWIN Project has developed, documented and implemented a risk management approach and plan based upon the SEI model. This approach supports analysis and quantification of impact using an "expert judgment" approach, categorizing both impact and probability on a scale of 1 – 3. This approach is included among the acceptable methods of risk quantification in IEEE Std 1490-1998 (PMBOK), section 11.2.2.5. The explanation of how probability and severity values are assigned are contained in the document CalWIN Risk Management Process (attached). Further detail is provided in the documents CalWIN Risk Management Process document and the monthly CalWIN Risk Management Plan (attached).

Other Consortiums

The standards for risk management planning are targeted at large software development efforts. C-IV will be required to provide risk management documentation that meets the above standards.

HHSDC SAWS Oversight is in the process of determining if this approach is appropriate and feasible for use in M&O (e.g., maintenance changes that exceed some predetermined size in estimated hours or cost). If it is determined this approach should be used in M&O the standards will be presented to the consortiums using the Transmission of State Expectations Process.